EXHIBIT 6

(June 17, 2021, Warrants)

Executed June 21, 2021

AO 93C (08/18)	Warrant by	Telephone or	Other Reliable	Electronic	Means

_	C	
-1	Origi	nal
_,	01151	Tirri

☐ Duplicate Original

UNITED STATES DISTRICT COURT

	for the	FIL	ED,
	District of Nevada	DA	TED: 3:07 pm, June 17, 2021
In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address) 487 E PETAL DEW AVENUE, LAS VEGAS, NEVADA 89183))) Case N))	U.S o. 2:21-mj-514-l	. MAGISTRATE JUDGE
WARRANT BY TELEPHON	E OR OTHER RELI	ABLE ELECT	RONIC MEANS
To: Any authorized law enforcement officer			
An application by a federal law enforcement of the following person or property located in the (identify the person or describe the property to be searched and Please see the Attachment A-1.		the government re District of	quests the search and seizure Nevada
I find that the affidavit(s), or any recorded described above, and that such search will reveal (ic Please see the Attachment B.			
YOU ARE COMMANDED to execute the in the daytime 6:00 a.m. to 10:00 p.m.		July 1, 2021 night because good	(not to exceed 14 days) cause has been established.
Unless delayed notice is authorized below, person from whom, or from whose premises, the pr property was taken.			
The officer executing this warrant, or an of as required by law and promptly return this warrant		Honorable D	ant, must prepare an inventory Daniel J. Albregts Magistrate Judge)
☐ Pursuant to 18 U.S.C. § 3103a(b), I find the § 2705 (except for delay of trial), and authorize the property, will be searched or seized (check the appropriate of the property). ☐ for	officer executing this war viate box) ne facts justifying, the later	nay have an adverse rant to delay notice	e result listed in 18 U.S.C.
☐ for days (not to exceed 30) ☐ until, the Date and time issued: June 17, 2021 2:34 p.s.	ALCT OF ACTION AND HONO	Judg	e's signature
City and state: Las Vegas, Nevada	HONORE HONOR	orable Daniel J. Albr	regts, U.S. Magistrate Judge
**	Manage Market Barrey St. Committee of the Committee of th		

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 3 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return			
Case No.: 2:21-mj-514-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:		
nventory made in the pres	ence of:			
nventory of the property t	aken and name(s) of any person(s) seized:			
	Certificatio	n.		
I declare under per designated judge.	nalty of perjury that this inventory is correct	and was returned along with the original warrant to the		
Date:				
Date:		Executing officer's signature		



SEALED

ATTACHMENT "A-1"

PREMISES TO BE SEARCHED - SUBJECT PREMISES 1

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

487 Petal Dew Avenue, Las Vegas, Nevada 89183 is a residential home leased by Paul ENGSTROM. Subject Premises is a two story, single family residence having primarily yellow beige stucco exterior with beige trim. The residence has a single car garage door that is beige in color and faces north. The numbers "487" are affixed to the east side of the residence above the garage. The front door of the residence is an unknown color encased by a white security door. Photo of Residence:



ATTACHMENT "B"

ITEMS TO BE SEIZED

2

3

4

5

6

7

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- Records concerning financial transactions associated with the operations or proceeds
 of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- f. Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

5

6

8

7

9 10

11 12

13

14

15

16

17

18

19

20

21

22

23 24

substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.

- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals. jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

1		documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2		instant messaging logs, photographs, and correspondence;
3	ii.	evidence of the presence or absence of software that would allow others to
4		control the device, such as viruses, Trojan horses, and other forms of
5		malicious software, as well as evidence of the presence or absence of security
6		software designed to detect malicious software;
7	iii.	evidence of the attachment of other devices;
8	iv.	evidence of counter-forensic programs (and associated data) that are designed
9		to eliminate data from the device;
10	v.	evidence of the times the device was used;
11	vi.	passwords, encryption keys, biometric keys, and other access devices that
12		may be necessary to access the device;
13	yii.	applications, utility programs, compilers, interpreters, or other software, as
14		well as documentation and manuals, that may be necessary to access the
15		device or to conduct a forensic examination of it;
16	viii.	records of or information about Internet Protocol addresses used by the
17		device;
18	ix.	records of or information about the device's Internet activity, including
19		firewall logs, caches, browser history and cookies, "bookmarked" or
20		"favorite" web pages, search terms that the user entered into any Internet
21		search engine, and records of user-typed web addresses.
22	2. As	s used herein, the terms "records," "documents," "programs," "applications,"
23	and "materials"	include records, documents, programs, applications, and materials created,
24		

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

- 1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.
- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- 4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

1	
2	
3	
4	
5	
6	the seiz
7	the
8	
9	aut info
10	info (f)(
11	cop
12	
13	invo seiz
14	phy stor
15	
16	foll
17	
18	
19	
20	
21	
22	
23	
24	

 h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

- 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:
- (e) Issuing the Warrant.
- (2) Contents of the Warrant.
- (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:
 - (i) execute the warrant within a specified time no longer than 14 days;
- (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.
 - (f) Executing and Returning the Warrant.
 - (1) Warrant to Search for and Seize a Person or Property.
- (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.
- Pursuant to this Rule, the government understands and will act in accordance with the following:
 - a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
 - b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

AO 93C (08/18)	Warrant by	Telephone	or Other 1	Reliable	Electronic	Means

_	A		
	Ori	oin	al
_	~ ~ ~	0	

☐ Duplicate Original

UNITED STATES DISTRICT COURT

	for the	FILED.	
	District of Nevada	DATED:	3:08 pm, June 17, 2021
In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address) 304 E. SILVERADO RANCH BOULEVARD UNIT 1110 LAS VEGAS, NEVADA 89183		U.S. MAC 2:21-mj-515-DJA	GISTRATE JUDGE
WARRANT BY TELEPHON	E OR OTHER RELIAE	BLE ELECTRO	NIC MEANS
To: Any authorized law enforcement officer			
An application by a federal law enforcement of the following person or property located in the (identify the person or describe the property to be searched and Please see the Attachment A-2.	Dis	government request strict of	s the search and seizure Nevada
I find that the affidavit(s), or any recorded described above, and that such search will reveal (id Please see the Attachment B.			eize the person or property
YOU ARE COMMANDED to execute the in the daytime 6:00 a.m. to 10:00 p.m. □	is warrant on or before at any time in the day or night	July 1, 2021 ht because good caus	(not to exceed 14 days) se has been established.
	at any time in the day or nig you must give a copy of the w	ht because good caus	se has been established. for the property taken to the
Unless delayed notice is authorized below, person from whom, or from whose premises, the presentation of the premises of the premise of the pr	at any time in the day or night you must give a copy of the wooperty was taken, or leave the	ht because good cause varrant and a receipt copy and receipt at	for the property taken to the the place where the nust prepare an inventory

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 17 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return			
Case No.: 2:21-mj-515-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:		
nventory made in the pres	ence of:			
nventory of the property t	aken and name(s) of any person(s) seized:			
	Certification	n .		
I declare under per designated judge. Date:	nalty of perjury that this inventory is correct	and was returned along with the original warrant to the		
Jaio,		Executing officer's signature		



SEALED

ATTACHMENT "A-2"

PREMISES TO BE SEARCHED – SUBJECT PREMISES 2

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

> 304 East Silverado Ranch Boulevard, Building 8, Apartment 1110, Las Vegas, Nevada 89183 is an apartment leased by Patricia ENGSTROM. Subject Premises is a two story, multi-family apartment building having a primarily tan stucco exterior with brown trim. The apartment has a single car garage door, on the north side of the building that is tan in color and faces north. The numbers "1110" are black in color on a white placard and is affixed to the right side of the front door. The front door of the residence is tan in color and faces the south. Photo of Residence:



ATTACHMENT "B"

ITEMS TO BE SEIZED

2

3

4

5

6

7

9

10 11

12

13

14

15

16

17

18

19

20

21

22

23

- 1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:
 - a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
 - b. Counterfeit controlled substances.
 - c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
 - d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
 - Records concerning financial transactions associated with the operations or proceeds
 of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.

- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals, jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

1		documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2		instant messaging logs, photographs, and correspondence;
3	ii.	evidence of the presence or absence of software that would allow others to
4		control the device, such as viruses, Trojan horses, and other forms of
5		malicious software, as well as evidence of the presence or absence of security
6		software designed to detect malicious software;
7	iii.	evidence of the attachment of other devices;
8	iv.	evidence of counter-forensic programs (and associated data) that are designed
9		to eliminate data from the device;
10	v.	evidence of the times the device was used;
11	vi.	passwords, encryption keys, biometric keys, and other access devices that
12		may be necessary to access the device;
13	yii.	applications, utility programs, compilers, interpreters, or other software, as
14		well as documentation and manuals, that may be necessary to access the
15		device or to conduct a forensic examination of it;
16	yiii.	records of or information about Internet Protocol addresses used by the
17		device;
18	ix.	records of or information about the device's Internet activity, including
19		firewall logs, caches, browser history and cookies, "bookmarked" or
20		"favorite" web pages, search terms that the user entered into any Internet
21		search engine, and records of user-typed web addresses.
22	2. As	s used herein, the terms "records," "documents," "programs," "applications,"
23	and "materials"	include records, documents, programs, applications, and materials created,
24		

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- 4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - f. scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

1	I	
À	I	
2	I	
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		

 h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

- 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:
- (e) Issuing the Warrant.
- (2) Contents of the Warrant.
- (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:
 - (i) execute the warrant within a specified time no longer than 14 days;
- (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.
 - (f) Executing and Returning the Warrant.
 - (1) Warrant to Search for and Seize a Person or Property.
- (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.
- 7. Pursuant to this Rule, the government understands and will act in accordance with the following:
 - a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
 - b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☐ Original

☐ Duplicate Original

UNITED STATES DISTRICT COURT

2 . 103 . 3	for the	FILED.	
	District of Nevada	DATED: 3	09 pm, June 17, 2021
In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address) 6145 HARRISON DRIVE, SUITE 4, LAS VEGAS, NEVADA 89120)	U.S. MAG	ISTRATE JUDGE
) Case N))	o. 2:21-mj-516-DJA	
WARRANT BY TELEPHON	E OR OTHER RELI	ABLE ELECTRONIC	C MEANS
Co: Any authorized law enforcement officer			
An application by a federal law enforcement of the following person or property located in the identify the person or describe the property to be searched an Please see the Attachment A-3.		the government requests the District of	he search and seizure Nevada
I find that the affidavit(s), or any recorded lescribed above, and that such search will reveal (in Please see the Attachment B.			e the person or property
YOU ARE COMMANDED to execute th	is warrant on or hefore	July 1, 2021	(not to exceed 14 days)
Barrior (1985) - 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	at any time in the day or		
Unless delayed notice is authorized below, person from whom, or from whose premises, the property was taken.			
The officer executing this warrant, or an of is required by law and promptly return this warran		ecution of the warrant, mus Honorable Daniel J.	
and the state of t		(United States Magistre	
☐ Pursuant to 18 U.S.C. § 3103a(b), I find the 2705 (except for delay of trial), and authorize the property, will be searched or seized (check the approp	officer executing this war	ant to delay notice to the p	
for days (not to exceed 30) until, t	he facts justifying, the later	specific date of	200
Date and time issued: June 17, 2021 2:34 p.m.	S Mental &	Judge's signal	ure
City and state: Las Vegas, Nevada	Maistrust SHono	orable Daniel J. Albregts, U Printed name an	S. Magistrate Judge
	WHAT THE THE PARTY OF THE PARTY	1 i inteu name un	a mit

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 31 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return				
Case No.: 2:21-mj-516-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:		
Inventory made in the presen	ce of:	·		
Inventory of the property take	en and name(s) of any person(s) seized:			
	Certification	on		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.				
Date:				
		Executing officer's signature		
		Printed name and title		



SEALED

ATTACHMENT "A-3"

PREMISES TO BE SEARCHED – SUBJECT PREMISES 3

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

6145 Harrison Drive Suite #4, Las Vegas, Nevada 89120 is a warehouse space primarily utilized by Paul ENGSTROM, Vincent CUOMO and Abraham ELLIOTT. Subject Premises is a single story, warehouse and suite having a primarily brown stucco exterior. The warehouse and suite has a single car rollup door that is beige in color and faces north. The number "4" is affixed to the glass front door just above eye level. The door of the warehouse and suite is glass with black trim and faces north. The address "6145 Harrison 1-12" is affixed to the north side of the building on the far-east side and is black in color. Photo of Warehouse and Suite:



ATTACHMENT "B"

ITEMS TO BE SEIZED

- 1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:
 - a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
 - b. Counterfeit controlled substances.
 - c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
 - d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
 - e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- f. Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- k. Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- 1. Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

- 1 2 3 4 5

- 10
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

- 2.2
- 23

24

- substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.
- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals. jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- t. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - i. evidence of who used, owned, or controlled the device at the time the things
 described in this warrant were created, edited, or deleted, such as logs,
 registry entries, configuration files, saved usernames and passwords,

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	and "
24	

- documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
- ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- iii. evidence of the attachment of other devices;
- iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
- v. evidence of the times the device was used;
- vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;
- vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
- viii. records of or information about Internet Protocol addresses used by the device;
- ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- 2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

- 1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.
- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- 4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - f. scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

23

24

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

- 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:
- (e) Issuing the Warrant.
- (2) Contents of the Warrant.
- (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:
 - (i) execute the warrant within a specified time no longer than 14 days;
- (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.
 - (f) Executing and Returning the Warrant.
 - (1) Warrant to Search for and Seize a Person or Property.
- (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.
- 7. Pursuant to this Rule, the government understands and will act in accordance with the following:
 - a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
 - b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☐ Original

☐ Duplicate Original

UNITED STATES DISTRICT COURT

	2 . 102.02	for the	71225555	FILED.	
		District of Neva	da	DATED: 3:09 pm	June 17, 2021
	In the Matter of the Search of	Y		U.S. MAGISTR	ATE JUDGE
	(Briefly describe the property to be searched or identify the person by name and address) 10388 MIDSEASON MIST STREET, LAS VEGAS, NEVADA 89183		Case No. 2:21-mj-5		
	WARRANT BY TELEPHON	E OR OTHER	RELIABLE ELE	CTRONIC M	EANS
o:	Any authorized law enforcement officer				
identify	An application by a federal law enforcement following person or property located in the with the person or describe the property to be searched and se see the Attachment A-4.		ney for the governme District of	ent requests the sea Nev	
	I find that the affidavit(s), or any recorded to bed above, and that such search will reveal (id) se see the Attachment B.				
	YOU ARE COMMANDED to execute this	s warrant on or befo	ore July 1,	2021 (not	to exceed 14 days)
V	in the daytime 6:00 a.m. to 10:00 p.m.	at any time in the	day or night because		
	Unless delayed notice is authorized below, a from whom, or from whose premises, the prety was taken.				
s requ	The officer executing this warrant, or an of uired by law and promptly return this warrant		Honora	warrant, must prep able Daniel J. Albre States Magistrate Judg	egts .
2705	Pursuant to 18 U.S.C. § 3103a(b), I find that (except for delay of trial), and authorize the try, will be searched or seized (check the appropriate)	officer executing th			
	for days (not to exceed 30) until, th	ne facts justifying, th	ne later specific date	of	1
Date a	I for days (not to exceed 30)	AL STED STATE		Judge's signature	100
City a	nd state: Las Vegas, Nevada	G MOISTANT	Honorable Daniel J	. Albregts, U.S. Ma Printed name and title	agistrate Judge
		The state of the s			

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 45 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return	
Case No.: 2:21-mj-517-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
nventory made in the pres	sence of :	-
nventory of the property t	caken and name(s) of any person(s) seized:	
	Certificatio	Ď.
I declare under per designated judge.	nalty of perjury that this inventory is correct	t and was returned along with the original warrant to the
Date:		
Date:		Executing officer's signature



SEALED

ATTACHMENT "A-4"

PREMISES TO BE SEARCHED – SUBJECT PREMISES 4

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

> 10388 Midseason Mist Street, Las Vegas, Nevada 89183 is the residential home of Abraham ELLIOTT. Subject Premises is a two story, single family residence having primarily beige stucco exterior with reddish brown trim. The residence has a single car garage door that is beige in color and faces west. The numbers "10388" are affixed to the south side of the residence above the garage. The front door of the residence is an unknown color encased by a white security door and faces west. Photo of Residence:



ATTACHMENT "B"

ITEMS TO BE SEIZED

13

14

15

16

17

18

19

20

21

22

23

- 1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:
 - a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
 - b. Counterfeit controlled substances.
 - c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
 - d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
 - e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.

- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals, jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

1		documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2		instant messaging logs, photographs, and correspondence;
3		ii. evidence of the presence or absence of software that would allow others to
4		control the device, such as viruses, Trojan horses, and other forms of
5		malicious software, as well as evidence of the presence or absence of security
6		software designed to detect malicious software;
7	i	ii. evidence of the attachment of other devices;
8		v. evidence of counter-forensic programs (and associated data) that are designed
9		to eliminate data from the device;
10		v. evidence of the times the device was used;
11		vi. passwords, encryption keys, biometric keys, and other access devices that
12		may be necessary to access the device;
13	v	ii. applications, utility programs, compilers, interpreters, or other software, as
14		well as documentation and manuals, that may be necessary to access the
15		device or to conduct a forensic examination of it;
16	vi	ii. records of or information about Internet Protocol addresses used by the
17		device;
18	118	ix. records of or information about the device's Internet activity, including
19		firewall logs, caches, browser history and cookies, "bookmarked" or
20		"favorite" web pages, search terms that the user entered into any Internet
21		search engine, and records of user-typed web addresses.
22	2.	As used herein, the terms "records," "documents," "programs," "applications,"
23	and "material	s" include records, documents, programs, applications, and materials created,
24		

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

 h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

- 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:
- (e) Issuing the Warrant.
- (2) Contents of the Warrant.
- (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:
 - (i) execute the warrant within a specified time no longer than 14 days;
- (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.
 - (f) Executing and Returning the Warrant.
 - (1) Warrant to Search for and Seize a Person or Property.
- (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.
- 7. Pursuant to this Rule, the government understands and will act in accordance with the following:
 - a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
 - b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

AO 93C (08/18)	Warrant by	Telephone	or Other 1	Reliable	Electronic	Means

_	A .		
1	Ori	oin	2
_,	O.L	5.11	

☐ Duplicate Original

UNITED STATES DISTRICT COURT

		for the	FILED	
		District of Nevada		3:10 pm, June 17, 2021
In the M	latter of the Search of)		GISTRATE JUDGE
or identify the 305 ST	be the property to be searched person by name and address) . AUGUSTINE LANE, RSON, NEVADA 89014)) Case N))	Jo. 2:21-mj-518-DJA	
WARR	ANT BY TELEPHO	NE OR OTHER REL	ABLE ELECTRON	IIC MEANS
To: Any authorized	l law enforcement officer			
of the following person	or property located in the ibe the property to be searched		r the government requests District of	s the search and seizure Nevada
	nat such search will reveal	ed testimony, establish proba		eize the person or property
	OMMANDED to execute		July 1, 2021	(not to exceed 14 days)
to an interest and		at any time in the day or		
		w, you must give a copy of the property was taken, or leave		
		officer present during the ex	ecution of the warrant, m Honorable Daniel	
as required by law and	promptly return this warra	ant and inventory to	(United States Magis	7
§ 2705 (except for dela property, will be search	y of trial), and authorize t	that immediate notification is the officer executing this war opriate box)	rant to delay notice to the	
for days	(not to exceed 30) until	, the facts his frying, the late	r specific date of	750
Date and time issued:	June 17, 2021 2:34 p.m	A MEDING	Judge's sign	nature V
City and state:	Las Vegas, Nevada	Thomas Right	orable Daniel J. Albregts,	U.S. Magistrate Judge
		the facts justifying, the late	Printed name	ana une

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 59 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return	
Case No.: 2:21-mj-518-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
inventory made in the pre-	sence of :	
nventory of the property	taken and name(s) of any person(s) seized:	
	Certificatio	n
I declare under pe designated judge.	nalty of perjury that this inventory is correct	t and was returned along with the original warrant to the
Date:		Executing officer's signature



SEALED

ATTACHMENT "A-5"

PREMISES TO BE SEARCHED - SUBJECT PREMISES 5

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

305 Saint Augustine Lane, Henderson, Nevada 89014 is a residential home leased by Virginia ENGSTROM. Subject Premises is a two story, single family residence having primarily beige stucco exterior with light brown trim. The residence has two separate garage doors that are beige in color and face east. The numbers "305" are affixed to the east side of the residence to the right side of the north garage door. The front door of the residence is brown in color and faces the east. Photo of Residence:



ATTACHMENT "B"

ITEMS TO BE SEIZED

2

3

4

6

7

8

9

10 11

12

13

14

15

16

17

18

19

20

21

22

23

24

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- Records concerning financial transactions associated with the operations or proceeds
 of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.

- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals, jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

1			documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2			instant messaging logs, photographs, and correspondence;
3		ii.	evidence of the presence or absence of software that would allow others to
4			control the device, such as viruses, Trojan horses, and other forms of
5			malicious software, as well as evidence of the presence or absence of security
6			software designed to detect malicious software;
7		iii.	evidence of the attachment of other devices;
8		iv.	evidence of counter-forensic programs (and associated data) that are designed
9			to eliminate data from the device;
.0		V.	evidence of the times the device was used;
1		vi.	passwords, encryption keys, biometric keys, and other access devices that
2			may be necessary to access the device;
3		vii.	applications, utility programs, compilers, interpreters, or other software, as
4			well as documentation and manuals, that may be necessary to access the
5			device or to conduct a forensic examination of it;
.6		viii.	records of or information about Internet Protocol addresses used by the
7			device;
8		ix.	records of or information about the device's Internet activity, including
9			firewall logs, caches, browser history and cookies, "bookmarked" or
20			"favorite" web pages, search terms that the user entered into any Internet
21			search engine, and records of user-typed web addresses.
22	2.	As	s used herein, the terms "records," "documents," "programs," "applications,"
23	and "mat	terials"	include records, documents, programs, applications, and materials created,
24			

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

- 1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.
- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- 4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

1 2 3 6. 4 (e) Issuing the Warrant. (2) Contents of the Warrant. 5 6 the officer to: 7 8 9 10 copying or review. 11 12 13 14 stored information that was seized or copied. 7. 15 following: 16 17 18 19 20 21 22 23 24

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

- Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:
- (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command
 - (i) execute the warrant within a specified time no longer than 14 days;
- (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site
 - (f) Executing and Returning the Warrant.
 - (1) Warrant to Search for and Seize a Person or Property.
- (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically
- Pursuant to this Rule, the government understands and will act in accordance with the
 - a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
 - b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☐ Original

☐ Duplicate Original

UNITED STATES DISTRICT COURT

OTHER S	TITLES DISTING	or cooki
	for the	FILED.
	District of Nevada	DATED: 3:58 pm, June 17, 2021
In the Matter of the Search of (Briefly describe the property to be searched	}	U.S. MAGISTRATE JUDGE
or identify the person by name and address) 2017 CHEVROLET SILVERADO (VIN: 3GCUKREC0HG108984) NEVADA LICENSE PLATE VMD601) Case No	o. 2:21-mj-519-DJA
WARRANT BY TELEPHON	E OR OTHER RELI	ABLE ELECTRONIC MEANS
Co: Any authorized law enforcement officer		
An application by a federal law enforcement of the following person or property located in the identify the person or describe the property to be searched an Please see the Attachment A-6.		the government requests the search and seizure District of Nevada
lescribed above, and that such search will reveal (id Please see the Attachment B.	lentify the person or describe the	property to be seized):
YOU ARE COMMANDED to execute the	is warrant on or hefore	July 1, 2021 (not to exceed 14 days)
Barrier (1984년 - 1984년		night because good cause has been established.
Unless delayed notice is authorized below, person from whom, or from whose premises, the property was taken.		e warrant and a receipt for the property taken to the the copy and receipt at the place where the
The officer executing this warrant, or an of is required by law and promptly return this warrant		ecution of the warrant, must prepare an inventory Honorable Daniel J. Albregts
		(United States Magistrate Judge)
Pursuant to 18 U.S.C. § 3103a(b), I find the 2705 (except for delay of trial), and authorize the property, will be searched or seized (check the appropriate)	officer executing this warr	
☐ for days (not to exceed 30) ☐ until, the	TO STRACE	specific date of
Date and time issued: June 17, 2021 2:34 p.m.	STATED INC.	Judge's signature
City and state: Las Vegas, Nevada	a Melatent Shono	rable Daniel J. Albregts, U.S. Magistrate Judge
	NOBE NOBE	Printed name and title
	The state of the s	

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 73 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return	
Case No.: 2:21-mj-519-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
inventory made in the pres	sence of :	-
nventory of the property	taken and name(s) of any person(s) seized:	
	Certificatio	o -
I declare under pe designated judge.		and was returned along with the original warrant to the
Date:		Executing officer's signature



SEALED

ATTACHMENT "A-6"

PREMISES TO BE SEARCHED - SUBJECT VEHICLE 1

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

2017 Chevrolet Pickup Truck, silver in color bearing Nevada license plate VMD601 VIN#3GCUKREC0HG108984. Current Registered Owner Vincent CUOMO, 487 Petal Dew Avenue, Las Vegas, Nevada 89183. Photo of vehicle:



ATTACHMENT "B" ITEMS TO BE SEIZED

2

3

4

6

7

8

10

9

11

12

13

14

15

16

17

18

19

20

21

22

23

24

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- Records concerning financial transactions associated with the operations or proceeds
 of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

3

4

5 6

7 8

9

10 11

12

13

14

15

16

17

18

19

20 21

22

23

- substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.
- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals. jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

1	1	documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2		instant messaging logs, photographs, and correspondence;
3	ii.	evidence of the presence or absence of software that would allow others to
4		control the device, such as viruses, Trojan horses, and other forms of
5		malicious software, as well as evidence of the presence or absence of security
6		software designed to detect malicious software;
7	iii.	evidence of the attachment of other devices;
8	iv.	evidence of counter-forensic programs (and associated data) that are designed
9		to eliminate data from the device;
10	V.	evidence of the times the device was used;
11	vi.	passwords, encryption keys, biometric keys, and other access devices that
12		may be necessary to access the device;
13	yii.	applications, utility programs, compilers, interpreters, or other software, as
14		well as documentation and manuals, that may be necessary to access the
15		device or to conduct a forensic examination of it;
16	viii.	records of or information about Internet Protocol addresses used by the
17	1	device;
18	ix.	records of or information about the device's Internet activity, including
19	9	firewall logs, caches, browser history and cookies, "bookmarked" or
20		"favorite" web pages, search terms that the user entered into any Internet
21	3	search engine, and records of user-typed web addresses.
22	2. As	used herein, the terms "records," "documents," "programs," "applications,"
23	and "materials" in	nclude records, documents, programs, applications, and materials created,
24		

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- 4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - f. scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

1 2 3 6. 4 (e) Issuing the Warrant. (2) Contents of the Warrant. 5 6 the officer to: 7 8 9 10 copying or review. 11 (f) Executing and Returning the Warrant. 12 13 14 stored information that was seized or copied. 7. 15 following: 16 17 18 19 20 21 22 23 24

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

- Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:
- (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command
 - (i) execute the warrant within a specified time no longer than 14 days;
- (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site
 - (1) Warrant to Search for and Seize a Person or Property.
- (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically
- Pursuant to this Rule, the government understands and will act in accordance with the
 - a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
 - b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

AO 93C (08/18)	Warrant by	Telephone or	Other Reliable	Electronic	Means

☐ Original

☐ Duplicate Original

UNITED	STATES	DISTRICT	COURT
CIVILLED	DIALDS	DISTRICT	COUNT

CMILD SI	MILO DISTRI		
	for the	FILED,	
	District of Nevada	DATED: 3:5	9 pm, June 17, 2021
In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address) 2007 BMW 328i (VIN: WBAVA33527KX79327) NEVADA LICENSE PLATE 12345TH)) Case I))	U.S. MAGI No. 2:21-mj-520-DJA	STRATE JUDGE
WARRANT BY TELEPHONE	OR OTHER REL	IABLE ELECTRONIC	MEANS
To: Any authorized law enforcement officer			
An application by a federal law enforcement of the following person or property located in the (identify the person or describe the property to be searched and g Please see the Attachment A-7.			search and seizure levada
I find that the affidavit(s), or any recorded test described above, and that such search will reveal (identification) Please see the Attachment B.			ne person or property
YOU ARE COMMANDED to execute this v in the daytime 6:00 a.m. to 10:00 p.m. □ a		July 1, 2021 r night because good cause has	not to exceed 14 days) been established.
Unless delayed notice is authorized below, yo person from whom, or from whose premises, the property was taken.	u must give a copy of	the warrant and a receipt for the	e property taken to the
The officer executing this warrant, or an office as required by law and promptly return this warrant ar		xecution of the warrant, must p Honorable Daniel J. Al (United States Magistrate.	bregts .
Pursuant to 18 U.S.C. § 3103a(b), I find that i § 2705 (except for delay of trial), and authorize the of property, will be searched or seized (check the appropriate days (not to exceed 30) until, the	ficer executing this wa	rrant to delay notice to the pers	
Date and time issued: June 17, 2021 2:34 p.m.	ALCT OF ARTHUR	Judge's signature	No
City and state: Las Vegas, Nevada	Facts justifying, the lat	norable Daniel J. Albregts, U.S. Printed name and ti	
	The same of the sa		

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 87 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return	
Case No.: 2:21-mj-520-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
inventory made in the pres	sence of :	
Inventory of the property t	taken and name(s) of any person(s) seized:	
	Certification	n.
I declare under pe designated judge.		n and was returned along with the original warrant to the
I declare under pe designated judge. Date:		



SEALED

ATTACHMENT "A-7"

PREMISES TO BE SEARCHED - SUBJECT VEHICLE 2

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

> 2007 BMW 4 door sedan, blue in color bearing Nevada license plate 12345TH VIN#WBAVA33527KX79327. Current Registered Owner Paul ENGSTROM, 487 Petal Dew Avenue, Las Vegas, Nevada 89183. Photo of vehicle:



ATTACHMENT "B"

ITEMS TO BE SEIZED

2

3

4

6

7

8

10

11

12

13

14

15

16

17

18

19

20

21

22

23

1.	The items to be seized are evidence, contraband, fruits, or instrumentalities of
violations o	f 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of
and Possess	ion with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit
Controlled S	Substance Offense), and 843(b) (Unlawful Use of a Communication Facility,
Including th	ne Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject
Offenses"),	namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- Records concerning financial transactions associated with the operations or proceeds
 of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

6

7 8

9

10 11

13

14

12

15

16

17 18

19

21

20

22

24

23

substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.

- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals. jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things
 described in this warrant were created, edited, or deleted, such as logs,
 registry entries, configuration files, saved usernames and passwords,

1		documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2		instant messaging logs, photographs, and correspondence;
3	ii.	evidence of the presence or absence of software that would allow others to
4		control the device, such as viruses, Trojan horses, and other forms of
5		malicious software, as well as evidence of the presence or absence of security
6		software designed to detect malicious software;
7	iii.	evidence of the attachment of other devices;
8	iv.	evidence of counter-forensic programs (and associated data) that are designed
9		to eliminate data from the device;
10	v.	evidence of the times the device was used;
11	vi.	passwords, encryption keys, biometric keys, and other access devices that
12		may be necessary to access the device;
13	yii.	applications, utility programs, compilers, interpreters, or other software, as
14		well as documentation and manuals, that may be necessary to access the
15		device or to conduct a forensic examination of it;
16	viii.	records of or information about Internet Protocol addresses used by the
17		device;
18	ix.	records of or information about the device's Internet activity, including
19		firewall logs, caches, browser history and cookies, "bookmarked" or
20		"favorite" web pages, search terms that the user entered into any Internet
21		search engine, and records of user-typed web addresses.
22	2. As	s used herein, the terms "records," "documents," "programs," "applications,"
23	and "materials"	include records, documents, programs, applications, and materials created,
24		

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

- 1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.
- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- 4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

24

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - f. scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

 h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

- 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:
- (e) Issuing the Warrant.
- (2) Contents of the Warrant.
- (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:
 - (i) execute the warrant within a specified time no longer than 14 days;
- (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.
 - (f) Executing and Returning the Warrant.
 - (1) Warrant to Search for and Seize a Person or Property.
- (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.
- 7. Pursuant to this Rule, the government understands and will act in accordance with the following:
 - a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
 - b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

4	0	93C	(08/18)	Warrant by	Telephone of	Other	Reliable	Electronic	Means

Original

☐ Duplicate Original

UNITED ST	ATES DIST	RICT COUF	RT	
	for the		FILED.	
	District of Nevad	a	DATED; 4:00 pm, June 17, 2021	
In the Matter of the Search of)		U.S. MAGISTRATE JUDGE	
(Briefly describe the property to be searched or identify the person by name and address) 2019 NISSAN ROGUE (VIN: 5N1AT2MT9KC7977 NEVADA LICENSE PLATE US263P) (93)))	ase No. 2:21-mj-5	o. 2:21-mj-521-DJA	
WARRANT BY TELEPHONE	OR OTHER R	ELIABLE ELE	CTRONIC MEANS	
To: Any authorized law enforcement officer				
An application by a federal law enforcement of the following person or property located in the (identify the person or describe the property to be searched and a Please see the Attachment A-8.		ey for the governme District of	ent requests the search and seizure Nevada	
I find that the affidavit(s), or any recorded test described above, and that such search will reveal (identification) Please see the Attachment B.				
YOU ARE COMMANDED to execute this in the daytime 6:00 a.m. to 10:00 p.m. □			2021 (not to exceed 14 days) good cause has been established.	
Unless delayed notice is authorized below, yo person from whom, or from whose premises, the propproperty was taken.				
The officer executing this warrant, or an offic as required by law and promptly return this warrant a		Honora	warrant, must prepare an inventory able Daniel J. Albregts States Magistrate Judge)	
Pursuant to 18 U.S.C. § 3103a(b), I find that § 2705 (except for delay of trial), and authorize the or property, will be searched or seized (check the appropria days (not to exceed 30) until, the	fficer executing this te box)	s warrant to delay n	otice to the person who, or whose	
Date and time issued: June 17, 2021 2:34 p.m.	TED STATE		Judge's signature	
City and state: Las Vegas, Nevada	facts justifying, the	Honorable Daniel J	. Albregts, U.S. Magistrate Judge Printed name and title	
	The Partition of the Pa			

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 101 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return	
Case No.: 2:21-mj-521-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
nventory made in the pres	ence of:	
nventory of the property t	aken and name(s) of any person(s) seized:	
	Certification	n
I declare under per designated judge.	nalty of perjury that this inventory is correct	and was returned along with the original warrant to the
Date:		Executing officer's signature
		Executing officer's signature Printed name and title



SEALED

ATTACHMENT "A-8"

PREMISES TO BE SEARCHED - SUBJECT VEHICLE 3

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

2019 Nissan SUV, silver in color bearing Nevada license plate US263P VIN#5N1AT2MT9KC797793. Current Registered Owner Paul ENGSTROM, 487 Petal Dew Avenue, Las Vegas, Nevada 89183. Photo of vehicle:



ITEMS TO BE SEIZED

ATTACHMENT "B"

20

21

22

23

- 1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:
 - a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
 - b. Counterfeit controlled substances.
 - c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
 - d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
 - e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

4 5

7 8

substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.

- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals, jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things
 described in this warrant were created, edited, or deleted, such as logs,
 registry entries, configuration files, saved usernames and passwords,

		documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
		instant messaging logs, photographs, and correspondence;
	ii.	evidence of the presence or absence of software that would allow others to
		control the device, such as viruses, Trojan horses, and other forms of
		malicious software, as well as evidence of the presence or absence of security
		software designed to detect malicious software;
	iii.	evidence of the attachment of other devices;
	iv.	evidence of counter-forensic programs (and associated data) that are designed
		to eliminate data from the device;
	V.	evidence of the times the device was used;
	vi.	passwords, encryption keys, biometric keys, and other access devices that
		may be necessary to access the device;
	vii.	applications, utility programs, compilers, interpreters, or other software, as
		well as documentation and manuals, that may be necessary to access the
		device or to conduct a forensic examination of it;
	viii.	records of or information about Internet Protocol addresses used by the
		device;
	ix.	records of or information about the device's Internet activity, including
		firewall logs, caches, browser history and cookies, "bookmarked" or
		"favorite" web pages, search terms that the user entered into any Internet
		search engine, and records of user-typed web addresses.
2.	As	used herein, the terms "records," "documents," "programs," "applications,"
and "mat	erials"	include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

24

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - f. scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate 1 and retrieve the evidence described in Attachment B. 2 Return and Review Procedures 3 Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part: 6. 4 (e) Issuing the Warrant. (2) Contents of the Warrant. 5 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be 6 seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: 7 (i) execute the warrant within a specified time no longer than 14 days; (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may 8 authorize the seizure of electronic storage media or the seizure or copying of electronically stored 9 information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and 10 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review. 11 (f) Executing and Returning the Warrant. (1) Warrant to Search for and Seize a Person or Property. 12 (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the 13 seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically 14 stored information that was seized or copied. Pursuant to this Rule, the government understands and will act in accordance with the 7. 15 following: 16 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of 17 the warrant, an agent is required to file an inventory return with the Court, that 18 is, to file an itemized list of the property seized. Execution of the warrant begins 19 when the United States serves the warrant on the named custodian; execution is 20 complete when the custodian provides all Search Warrant Data to the United 21 States. Within fourteen (14) days of completion of the execution of the warrant, 22 the inventory will be filed. 23 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which 24 the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

Original

☐ Duplicate Original

LIMITED STATES DISTRICT COLDT

	UNITED 5	IATES DIST	RICI COU	KI	
		for the		FILED.	
		District of Nevad	a	DATED: 4:01 pt	m, June 17, 2021
In the M	atter of the Search of)		U.S. MAGISTI	RATE JUDGE
or identify the p	e the property to be searched person by name and address) S (VIN: 1G6AR5SS3G01956 CENSE PLATE AL7456		se No. 2:21-mj-522-DJA		
WARRA	ANT BY TELEPHONE	OR OTHER R	ELIABLE EI	ECTRONIC	MEANS
To: Any authorized	law enforcement officer				
of the following person	by a federal law enforcement or property located in the the the property to be searched and ment A-9.	7 6 66 7 7	ey for the govern District of		search and seizure Nevada
	fidavit(s), or any recorded te at such search will reveal (ide ment B.				the person or property
	MMANDED to execute this :00 a.m. to 10:00 p.m.	warrant on or befor at any time in the d			(not to exceed 14 days) s been established.
	notice is authorized below, y rom whose premises, the pro				
	outing this warrant, or an officeromptly return this warrant a		Hono	orable Daniel J. A	Albregts
- Alamania		A 100 may 200		ed States Magistrate	
§ 2705 (except for delay property, will be searched	J.S.C. § 3103a(b), I find that of trial), and authorize the ced or seized (check the appropriation to exceed 30) until, the	fficer executing this te box)	s warrant to delay	notice to the per	
Date and time issued:	June 17, 2021 2:34 p.m.	ALCT OF ANTINE		Judge's signatur	W .
City and state: _L	as Vegas, Nevada	facts justifying, the	Honorable Danie	J. Albregts, U.S Printed name and t	. Magistrate Judge
		The state of the s			

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 115 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return	
Case No.: 2:21-mj-522-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
inventory made in the pre	sence of:	
Inventory of the property	taken and name(s) of any person(s) seized:	
	Certification	n.
I declare under pe designated judge.		
I declare under pe designated judge. Date:		and was returned along with the original warrant to the Executing officer's signature



SEALED

ATTACHMENT "A-9"

PREMISES TO BE SEARCHED - SUBJECT VEHICLE 4

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

2016 Cadillac 4 door CTS, gray in color bearing Nevada license plate AL7456 VIN#1G6AR5SS3G0195627. Current Registered Owner Abraham ELLIOTT, 10388 Midseason Mist Street, Las Vegas, Nevada 89183. Photo of vehicle:



ATTACHMENT "B"

ITEMS TO BE SEIZED

2

3 4

5

6

7

8

9

10

11

12

13 14

15

16

17

18

19

20

21

22

23

24

The items to be seized are evidence, contraband, fruits, or instrumentalities of 1. violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- f. Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

4 5

substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.

- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals, jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- u. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

		documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
		instant messaging logs, photographs, and correspondence;
	ii.	evidence of the presence or absence of software that would allow others to
		control the device, such as viruses, Trojan horses, and other forms of
		malicious software, as well as evidence of the presence or absence of security
		software designed to detect malicious software;
	iii.	evidence of the attachment of other devices;
	iv.	evidence of counter-forensic programs (and associated data) that are designed
		to eliminate data from the device;
	V.	evidence of the times the device was used;
	vi.	passwords, encryption keys, biometric keys, and other access devices that
		may be necessary to access the device;
	vii.	applications, utility programs, compilers, interpreters, or other software, as
		well as documentation and manuals, that may be necessary to access the
		device or to conduct a forensic examination of it;
	viii.	records of or information about Internet Protocol addresses used by the
		device;
	ix.	records of or information about the device's Internet activity, including
		firewall logs, caches, browser history and cookies, "bookmarked" or
		"favorite" web pages, search terms that the user entered into any Internet
		search engine, and records of user-typed web addresses.
2.	As	used herein, the terms "records," "documents," "programs," "applications,"
and "mat	erials"	include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

-77

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

- 1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.
- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- 4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

24

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - f. scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate 1 and retrieve the evidence described in Attachment B. 2 Return and Review Procedures 3 Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part: 6. 4 (e) Issuing the Warrant. (2) Contents of the Warrant. 5 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be 6 seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: 7 (i) execute the warrant within a specified time no longer than 14 days; (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may 8 authorize the seizure of electronic storage media or the seizure or copying of electronically stored 9 information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and 10 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review. 11 (f) Executing and Returning the Warrant. (1) Warrant to Search for and Seize a Person or Property. 12 (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the 13 seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically 14 stored information that was seized or copied. Pursuant to this Rule, the government understands and will act in accordance with the 7. 15 following: 16 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of 17 the warrant, an agent is required to file an inventory return with the Court, that 18 is, to file an itemized list of the property seized. Execution of the warrant begins 19 when the United States serves the warrant on the named custodian; execution is 20 complete when the custodian provides all Search Warrant Data to the United 21 States. Within fourteen (14) days of completion of the execution of the warrant, 22 the inventory will be filed. 23 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which 24 the electronically stored information must be seized after the issuance of the

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☐ Original

☐ Duplicate Original

UNITED STATES DISTRICT COURT

	OTHER	D STITLES DISTI	CICT COCICT	- D	
		for the	FILI		
		District of Nevada	DA	TED: 4:01 pm, June 17, 2021	
(Briefly descr or identify th 2015 (VIN: 1	In the Matter of the Search of (Briefly describe the property to be search or identify the person by name and addres		U.S. e No. 2:21-mj-523-	U.S. MAGISTRATE JUDGE 21-mj-523-DJA	
	2015 CHEVROLET SONIC (VIN: 1G1JC6SG4F4213150) NEVADA LICENSE PLATE 579NO	08			
	WARRANT BY TELEPH	IONE OR OTHER RE	LIABLE ELECT	RONIC MEANS	
o:	Any authorized law enforcement offic	er			
identify	An application by a federal law enforce following person or property located in the person or describe the property to be searches see the Attachment A-10.	the	for the government re District of	quests the search and seizure Nevada	
	I find that the affidavit(s), or any recorded above, and that such search will reveale see the Attachment B.				
	YOU ARE COMMANDED to execu	te this warrant on or before	July 1, 2021	(not to exceed 14 days)	
V	in the daytime 6:00 a.m. to 10:00 p.m.	at any time in the day	or night because good	d cause has been established.	
	Unless delayed notice is authorized be from whom, or from whose premises, to was taken.				
s requ	The officer executing this warrant, or a tired by law and promptly return this wa		Honorable I	Daniel J. Albregts Magistrate Judge)	
2705 propert	Pursuant to 18 U.S.C. § 3103a(b), I fin (except for delay of trial), and authorizety, will be searched or seized (check the approximately) for days (not to exceed 30) ur	e the officer executing this v	varrant to delay notice		
Date ar	nd time issued: June 17, 2021 2:34 p	o.m. WIED STATES OF STREET	Judg	re's signature	
City an	nd state: Las Vegas, Nevada	WOOSE SHE	enorable Daniel J. Alb	regts, U.S. Magistrate Judge I name and title	
		The state of the s			

Case 2:21-cr-00190-ART-EJY Document 238-6 Filed 05/22/23 Page 129 of 141

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

	Return	
Case No.: 2:21-mj-523-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
inventory made in the pre-	sence of :	
nventory of the property	taken and name(s) of any person(s) seized:	
	Certificatio	n.
I declare under pe designated judge.	nalty of perjury that this inventory is correct	t and was returned along with the original warrant to the
Date:		Executing officer's signature



SEALED

ATTACHMENT "A-10"

PREMISES TO BE SEARCHED - SUBJECT VEHICLE 5

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

> 2015 Chevrolet 4 door hatchback, black in color bearing Nevada license plate 579N08 VIN#1G1JC6SG4F4213150. Current Registered Owner Joseph KRIEGER, 6144 Camino De Rosa Drive #3, Las Vegas, Nevada 89108. Photo of vehicle:



ATTACHMENT "B"

2

3

4

5

6

7

8

9

10

11

12 13

14

15

16

17

18

19

20

21

22

23

24

ITEMS TO BE SEIZED

- The items to be seized are evidence, contraband, fruits, or instrumentalities of 1. violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:
 - a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
 - b. Counterfeit controlled substances.
 - c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
 - d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
 - e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- digital account opening documents, statements, deposit slips, checkbooks, orders or confirmations of wire transfers.
- f. Records of any accounts or transactions within the traditional banking or credit systems or via cryptocurrencies.
- g. Digital currency, cryptocurrency (or digital currency) private keys, and digital currency recovery seeds, as further explained in paragraph 4 below.
- h. Packing material or inserts relating to any transactions with any cash-forcryptocurrency exchange.
- i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential co-conspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances.
- j. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners, not to exceed 15 items for any residence.
- Records concerning the use of commercial mail receiving agencies and/or post office boxes.
- Photographs and/or videotapes, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled

4 5

substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators.

- m. Records relating to the use of and accumulation of proceeds derived from the sale of illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including precious metals, jewelry, records of large purchases, receipts, keys and other items tending to establish dominion and control of the location, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts.
- n. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses.
- o. Financial records of persons in control of the property, premises, or vehicles, including bank statements, bank receipts, passbooks, bank checks, money market or similar accounts, money drafts, letters of credit, payroll documents, employer information, income and expense records, Federal and State income tax returns, money orders, cashier's checks, loan applications, credit card records, safe deposit box and records, acquisitions, notes, and records reflecting vehicles, aircraft or vessels owned, purchased, sold or leased.

- p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- q. United States currency in excess of \$2,000, including the first \$2,000 if more than \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- r. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures.
- s. Paraphernalia for packaging, processing, cutting, weighing, and distributing controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.
- With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - evidence of who used, owned, or controlled the device at the time the things
 described in this warrant were created, edited, or deleted, such as logs,
 registry entries, configuration files, saved usernames and passwords,

		documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
		instant messaging logs, photographs, and correspondence;
	ii.	evidence of the presence or absence of software that would allow others to
		control the device, such as viruses, Trojan horses, and other forms of
		malicious software, as well as evidence of the presence or absence of security
		software designed to detect malicious software;
	iii.	evidence of the attachment of other devices;
	iv.	evidence of counter-forensic programs (and associated data) that are designed
		to eliminate data from the device;
	V.	evidence of the times the device was used;
	vi.	passwords, encryption keys, biometric keys, and other access devices that
		may be necessary to access the device;
	vii.	applications, utility programs, compilers, interpreters, or other software, as
		well as documentation and manuals, that may be necessary to access the
		device or to conduct a forensic examination of it;
	viii.	records of or information about Internet Protocol addresses used by the
		device;
	ix.	records of or information about the device's Internet activity, including
		firewall logs, caches, browser history and cookies, "bookmarked" or
		"favorite" web pages, search terms that the user entered into any Internet
		search engine, and records of user-typed web addresses.
2.	As	used herein, the terms "records," "documents," "programs," "applications,"
and "mat	erials"	include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- 3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds shall also be construed to include seizure of any cryptocurrency related to any such seized private keys and/or recovery seeds, and such seizure shall allow transfer of any such related cryptocurrency to one or more government controlled accounts, or "wallets."

ATTACHMENT "C" PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

- 1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.
- 2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.
- 3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.
- Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate Court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

- 5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
 - f. scanning storage areas;
 - g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate 1 and retrieve the evidence described in Attachment B. 2 Return and Review Procedures 3 Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part: 6. 4 (e) Issuing the Warrant. (2) Contents of the Warrant. 5 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be 6 seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: 7 (i) execute the warrant within a specified time no longer than 14 days; (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may 8 authorize the seizure of electronic storage media or the seizure or copying of electronically stored 9 information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and 10 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review. 11 (f) Executing and Returning the Warrant. (1) Warrant to Search for and Seize a Person or Property. 12 (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the 13 seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically 14 stored information that was seized or copied. Pursuant to this Rule, the government understands and will act in accordance with the 7. 15 following: 16 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of 17 the warrant, an agent is required to file an inventory return with the Court, that 18 is, to file an itemized list of the property seized. Execution of the warrant begins 19 when the United States serves the warrant on the named custodian; execution is 20 complete when the custodian provides all Search Warrant Data to the United 21 States. Within fourteen (14) days of completion of the execution of the warrant, 22 the inventory will be filed. 23 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which 24 the electronically stored information must be seized after the issuance of the 57

24

warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

- c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;
- d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.
- e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, that information will be copied onto appropriate media and returned to the person from whom the information was seized.